

Amendments to the Specification

Please replace the paragraph on Page 8, lines 14-17 with the following marked-up replacement paragraph:

-- Accordingly, what is needed is a technique for providing consistent, end-to-end protection for user datagrams throughout the network path they travel, whether over secure or non-secure networks, while still allowing the packet ~~context~~ content to be surfaced in cleartext form in security gateways. --

Please replace the paragraph on Page 9, lines 4-5 with the following marked-up replacement paragraph:

-- Another object of the present invention is to provide this technique in a manner that allows the packet ~~context~~ content to be surfaced in cleartext form in security gateways. --

Please replace the paragraph on Page 19, lines 5-14 with the following marked-up replacement paragraph:

-- As stated earlier, security breaches may occur once a data packet enters the intranet environment of Fig. 3 because the data is transmitted in un-encrypted, un-protected form. Fig. 4 illustrates the improved remote access environment provided when using the present invention, whereby this security concern has been addressed. To transmit data between remote host 405 and server 440, through intermediate security gateway ~~[[425]]~~ 420, two secure tunnels are now used. Tunnel 1 (element 415) securely transports data through the Internet 410, in a manner

similar to that of the tunnel 315 in Fig. 3. Tunnel 2 (element 435) provides secure transport through the intranet 430. Security gateway 420 still has access to the data in cleartext form when using these two tunnels, retaining the ability to provide services (represented by element 425) of the type which were available in the environment of Fig. 3. —

Please replace the paragraph on Page 21, lines 6-14 with the following marked-up replacement paragraph:

-- The improved business partner computing environment provided when using the present invention is shown in Fig. 8. As in Fig. 6, three cascaded tunnels 815, 835, 855 are established. Business partner A 805 securely transmits data through network 810 (which may be the Internet or an intranet) to security gateway 820 using the first tunnel 815. ~~815, which Security gateway 820~~ securely transmits data through the Internet 830 to security gateway 840 using the second tunnel 835, and security gateway 840 securely transmits the data through network 850 (which may be the Internet or an intranet) to business partner B 860 using the third tunnel 855. End-to-end data protection is thereby provided, while still enabling content inspection services (~~illustrated~~illustrated as elements 825, 845) to be performed in the security gateways using the cleartext content of the data packets. —

Please replace the paragraph on Page 23, lines 8-9 with the following marked-up replacement paragraph:

-- • Client 905 will fill the role of "IKE Initiator" for both Phase 1 and Phase 2

Serial No. 09/754,893

3

RSW920000162US1

negotiations with the gateway for tunnel pair 1 (shown at 910, 915) --

Please replace the paragraph on Page 25, lines 1-21 with the following marked-up replacement paragraph:

-- • When a data packet arrives from the client at the gateway, the gateway can decrypt that packet using the decryption key corresponding to the IPSec SA (see element 915 of Fig. 9) established with the client on the tunnel 1 side. At this point in the process, the gateway is in possession of a cleartext copy of a datagram addressed from 9.1.2.3 to 8.1.2.3. In the prior art, the gateway would simply process this datagram as a conventional datagram to be forwarded. However, it is desirable to continue protecting the datagram on its next network segment. Thus, the present invention enables additional security policy information to be used wherein the datagram will be forwarded on a secure cascaded tunnel on the tunnel 2 side of the gateway. The present invention therefore provides an additional element in the specification of the IKE/IPSec policy (to be stored in the gateway's ingress and egress SPDs 1010, 1035) that will direct the gateway to either use an existing cascaded tunnel, or if one is not available, to establish a pair of IKE and IPSec security associations that will provide this next cascaded tunnel. This additional policy element is specified in the form of a "cascading-enabled" flag which will be included in the security associations identified by the SPIs already established for each direction of transmission. When the cascading-enabled flag is set on, this indicates that the datagram is to be sent on a cascaded tunnel as it leaves the gateway's egress interface. Because the IDci and IDcr payloads are identical for each direction of transmission, the inclusion of an identical "cascading-

Serial No. 09/754,893

4

RSW920000162US1

enabled" flag in the security associations for both ~~direction~~ directions of transmission will also handle the cascading of SA tunnels for traffic flowing in the opposite direction, from server 935 to client 905. --

Serial No. 09/754,893

5

RSW920000162US1